IT Security Procedural Guide: Salesforce Platform Security Implementation CIO-IT Security-11-62

Revision 2.5

February 26, 2020

Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
Version 1.x				
1.	Jan Schober Booz Allen Hamilton	Draft version 1.1 – • Added User Permission File attachment; • Updated Application Approval Process • Added Application Security Form and rearranged process steps	ISSM direction	P12 P7 P7
2.	Jan Schober Booz Allen Hamilton	Draft version 1.2 • Updated Application Approval Process, step 5. • Updated Application Security Assessment Form	ISSM direction	P7 P7
3.	Jan Schober Booz Allen Hamilton	Draft version 1.3 • Addressed PBS provided comments • Updated Application Approval Process PIA and Application Security Assessment Forms	ISSM direction	P1 P2 P 6 P8
4.	Jan Schober Booz Allen Hamilton	Draft version 1.4 • Updates made to section 2.2.1 • Updates made to section 2.2.3, GSA NIST 800-53 Controls Spreadsheet file • Updates made to section 2.2.2 Application Approval Process file ○ COE Process Flow ○ Section 2, Step 5 • Added Organization Baseline Security Configuration Settings file to section 2.2.4	ISSM direction	P7 P8
5.	Jan Schober Booz Allen Hamilton	Draft version 1.5 • Inserted Updated Baseline Security Configuration Settings Reference Guide file into section 2.2.4 • Inserted Security Controls Analysis file into Application Approval Process, Step 4.	ISSM direction	P8 P6
6.	Blanche Heard	Draft version 1.5 • Accepted stakeholder comments/revisions	OSAISO-stakeholder review	Various
Version 2.x				
7.	Peter Nichols	Draft version 2.1 • Inserted Scanning Methodology in Section 9. • Corrected various grammatical/typographical errors. • Updated Application Review document. • Inserted Customer Access Methodology in Section 10. • Updated Section 8	ISSM direction	Various

8.	Amy Reecer Booz Allen Hamilton	Draft version 2.2 • Inserted updated timeout screenshot. • Inserted Customer Chatter Groups w/External Access in Section 11.	ISSM direction	P12 P15 & P16
9.	Peter Nichols	Draft version 2.3 • Update to Sub-System Application Approval Process Document • Update to Application Review Checklist	ISSM direction	
10.	Blanche Heard	• IT Security POC/Stakeholder comments	OSAISO direction	Various
11.	Peter Nichols	• had a screen timeout setting of 30 min...when it should now be 60....	ISSM direction	Section 4.9 screen shot
12.		• Changes made throughout the document to reflect NIST and GSA requirements	Regular Update	Various
13.	John Sitcharing	• Included update of Rev 4 800-53 NIST controls and GSA requirements for procedural guide 06-30	Regular Update	Various
14.	Dan Stanfield	Version 2.4 • Included updates related to SF App security	Regular Update	Various
15.	Dean/ Klemens	Version 2.5 • Updated style and formatting structure to align with current practices. • Renamed guide. • Updated Points of Contact	Regular Update	Various

Approval

IT Security Procedural Guide: Salesforce Platform Security Implementation, CIO-IT Security-11-62 Version 2.5 is hereby approved for distribution.

X

Bo Berlas
Acting GSA Chief Information Security Officer

Contact:

Concerning this guide - GSA Office of the Chief Information Security Officer (OCISO), Policy and Compliance Division (ISP), at ispcompliance@gsa.gov.

Concerning GSA Salesforce and Salesforce processes - GSA OCISO Information Systems Security Officer (ISSO) Support Division Application Support Team at app-support@gsa.gov.

Table of Contents

1 Introduction

General Services Administration (GSA) has the capability to utilize commercial cloud computing services provided appropriate security controls are implemented, tested, and reviewed as part of the agency's information security program. These services are protected to the degree required by Federal Information Security Modernization Act (FISMA), FISMA implementing standards, and the most current GSA guidance. The Salesforce Platform as a Service (PaaS) and Software as a Service (SaaS) cloud computing offerings have unique attributes and require consistent risk management and continuous monitoring processes. While the basic Assessment and Authorization (A&A) procedures do not change, Salesforce represents a new model for Information Technology (IT) development by offering extensive options for configuring workflows, databases, forms, dashboards and reports, process modeling, and customizable user interfaces. As a cloud solution, the Salesforce application configurations can take place without any requirements for hardware or software. In addition the Salesforce platform, Force.com, offers two extremely valuable features by supporting mobile access and social business collaboration all from within the platform itself. Salesforce supports a standard method of application development therefore the potential for sharing and using the work of the entire GSA development community is immense.

Salesforce enables GSA to quickly and efficiently build applications to modernize our IT portfolio and promote innovative solutions in the areas of mobility, employee collaboration, shared development efforts and customer relationship management integration. Additional information on Salesforce can be viewed at the Salesforce security wiki –

http://wiki.developerforce.com/index.php/Security

2 Purpose

This guide assists GSA employees and contract personnel that have IT Security responsibilities, implement a standard Salesforce Assessment and Authorization. The guide outlines the key activities for implementing the process.

3 Assumptions

- The procedures and policies outlined in this guide are incorporated into the Center of Excellence (COE) for GSA.
- Salesforce organizations are maintained by OCIO.
- Mandatory customer implemented organizational level settings identified in this guide are configured on all Salesforce organizations.
- Mandatory customer implemented application level settings identified are configured on all applications published on the Salesforce platform.
- Applications developed for internal GSA use are enabled with authentication and will use SSO. Access to these applications must be allowed from any location.
- Applications developed for external GSA use must have authentication enabled as deemed appropriate by the Business Owner and Authorizing Official (AO).

- All applications developed will be reviewed and approved for IT security requirements as outlined in this guide. Coordination will occur between the ISSO and ISSM in this process.
- Organization and Application Administrators are designated by the AO.

4 GSA Salesforce Methodology

4.1 Definitions and Concepts

The following sections describe a Salesforce Organization, Application and GSA Salesforce customers.

4.2 Salesforce Organization

Saleseforce.com, Inc. provides the Force.Com Platform as a Service (PaaS). The platform allows GSA developers to create and define unique "Org" instances in which individual subsystems (previously called minor apps) are created.

These applications are built using Apex and Visualforce. AppExchange is a marketplace for cloud computing applications built for the Salesforce.com community and delivered by partners or by third-party purchased developer services, which users can purchase or download for free and add to their Salesforce.com environment.

4.3 GSA Salesforce Customers

The following GSA Salesforce Customer Organizations are designed to meet the unique business requirements described:

- Enterprise Engagement Org (EEO) - Focuses on GSA's role as an employer, supporting internal GSA collaboration and productivity.
- Public Engagement Org (PEO) - Focuses on GSA's role as a citizen resource by hosting the Federal Citizens Information Center, a citizen-facing call center for USA.gov and other government agency websites.
- Government Engagement Org (GEO) - Focuses on GSA's role as a government coordinator, supporting cross-government policy initiatives and data collection efforts.
- PBS Client Solutions Org (CS) - Focuses on GSA's role as a leasing organization, coordinating Public Buildings Service customer relationships and overseeing services to customers.
- Property Disposal Org (PD) - Focuses on GSA's role as a property manager, supporting the repositioning of unneeded government real property.
- Workspaces Org (WS) - Focuses on GSA's role as a property manager, providing workspace project management tools as well as a mechanism for allowing people and businesses to lease space to the government.
- Customer Engagement Org (CEO) - Focuses on GSA's role as a customer-facing sales organization by facilitating marketing, customer service, and sales activities for the

Federal Acquisitions Service, as well as other GSA customer-centric forums and activities.

4.4 Salesforce Subsystem Customization

GSA Salesforce application customization will be done at the "*Organization*" level by adding customized applications to a Salesforce Organization. This includes adding sets of customized tabs for specific vertical- or function-level (Finance, Human Resources, etc.) features.

4.5 Salesforce Assessment and Authorization Process

System Owners are responsible for ensuring that Salesforce Organizations and Applications have been through the applicable GSA security Assessment and Authorization process and have received Authorization to Operate (ATO). The approval process for both Organizations and Applications is described in the subsections below.

4.6 Organization Security Approval Process

A Salesforce Organization requires an Authority to Operate within GSA. At the discretion of the AO, a new Assessment and Authorization can be done or the system environment description and security control analysis can be integrated into an existing Assessment and Authorization package. The security approval process is the responsibility of the System ISSO working with the ISSM, Business Owner, System Development Team and the CISO office. Refer to the latest GSA CIO-IT Security-06-30, *“Managing Enterprise Risk”*, for a description of the GSA agency-wide Assessment and Authorization process and key activities.

The security controls analysis is performed using the latest NIST 800-53 Controls for Salesforce worksheet provided in section 4.8. The remainder of the process is the same as identified in the transmittal letter for an Assessment and Authorization package:

- SSP (reference customer implemented controls as appropriate from the Cloud Salesforce Assessment and Authorization)
- PIA (submit the completed draft to the Privacy Office during application development and submit the completed final to the Privacy Officer for signature prior to application deployment)
- SAR
- Authorization Decision Letter
- POA&M

4.7 Application Approval Process

The security approval process for Salesforce applications is the responsibility of the System ISSO working with the Business Owner, System Application Development Team and the CISO office. The first step is to determine the type of application. If the application is a Major Application, then a full Assessment and Authorization is required.

If the application is determined to be a Subsystem Application, new application development will require a security package. Many application revisions will also either require an update to the Subsystem Application security package, or else in-development verifications by security personnel (security review). The following reference provides a specific delineation table showing what degree of security involvement is required, based on the Subsystem application revisions which are being applied to any given iterative change. Note, resolution types can be found at the following link.

Resolution Types w/Associated Approval and Tier Levels

If a security package is required, there are key activities that should be completed. The "GSA Implementation of Security for Salesforce Subsystems" is available at the link below and provides the steps required during the Subsystem approval process.

Implementation of Subsystems

4.8 GSA NIST 800-53 Controls for Salesforce

The link below contains the most current NIST 800-53 Controls for Salesforce Worksheet. It provides the baseline security controls for a Salesforce Organization as well as the controls for an Application. The table identifies a control as inherited, common or hybrid control, or required to be implemented at the Organization or Application level. The worksheet available at the link below can be adjusted based on the GSA S/SO or contractor's environment to address specific mission or business requirements, priorities, or customized conditions. Conduct a security control analysis using the worksheet, and document the selected security controls. The completed worksheet should be included in the appendices section of the SSP. It must be updated in subsequent steps of the risk management process.

Salesforce Guide 11-62 Section 4 8 Controls

4.9 Salesforce Organization Baseline Security Configuration Settings

When a GSA customer uses a Salesforce Organization or Application, there are certain configuration responsibilities that must be implemented. These are the customer security configurations that allow the cloud services to integrate properly and securely with GSA systems. The recommended security configuration settings to be applied to Salesforce Organizations and Applications are provided in the Salesforce Organization Baseline Security Configuration Reference Guide available at the link below. It is the responsibility of the system ISSO to ensure periodic monitoring (weekly, monthly or quarterly as per the direction of the AO and/or ISSM) of the configuration settings at the Organization and Application level.

Example Salesforce Organization Baseline

5 Salesforce Security Configuration Options Parameters

The Salesforce Security Configuration Options Parameters present the configurable user settings available to Organization Administrators (see the document at the link below). These parameters can also be used to further harden an Organization and subsequent Application for users. Some settings are included in the Salesforce Organization Baseline Security Configuration Reference Guide. Care should be used to analyze these controls before implementation to ensure that the customer implemented controls are not affected. Any deviations to these settings must be documented in a Business Process Document (BPD) for the Org affected.

Salesforce Security Settings

6 Salesforce Security Best Practices

A key activity of application development and system configuration is access security. Security measures should not only protect data and logic from unauthorized external access, but also from unauthorized internal access. The Salesforce Security Best Practices available at the link below includes guidance for configuration settings and features that will ensure sufficient data protection.

Salesforce Security Implementation Guide

7 Salesforce Profile Management Overview

Force.com provides a layered security framework that allows security administrators to create profiles, permission sets, roles, hierarchies and rules that are enforced in the user interface. GSA uses Permission Sets to grant access to tabs and objects for a given application. To specify the fields a user can access, the administrator uses field-level security. To specify the individual records a user can view and edit, the administrator sets organization-wide defaults, defines a role hierarchy, and creates sharing rules. The Salesforce Guide to Sharing Architecture available at the link below describes detailed concepts of the Salesforce security data access model. For further information about the access model and hands-on training, ISSO’s are encouraged to complete the following Salesforce security courses:

- Salesforce Data Security
- Salesforce Secure Identity and Access Management
- A Guide to Sharing Architecture

7.1 Salesforce Navigation Tips

To access Salesforce Security configurations select the "Setup" choice from the pull down menu below the userid name.

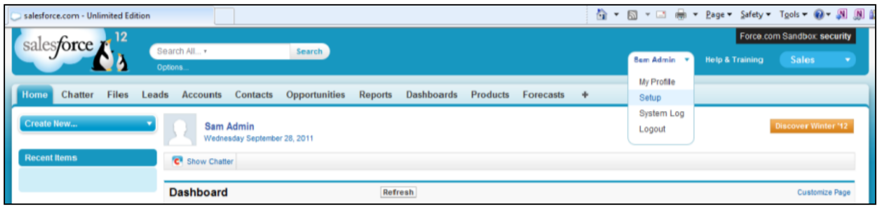
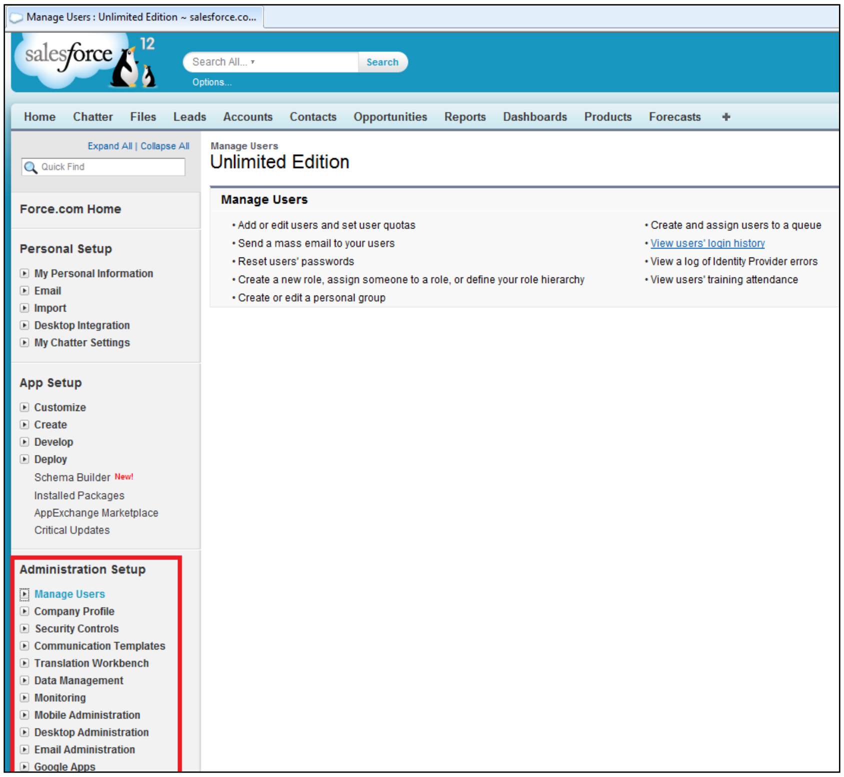


Figure 7-1 Setup Pull Down Menu

The Administration Setup configuration family is available only to organization administrators.



Manage Users

Unlimited Edition

Manage Users

- Add or edit users and set user quotas
- Send a mass email to your users
- Reset users' passwords
- Create a new role, assign someone to a role, or define your role hierarchy
- Create or edit a personal group
- Create and assign users to a queue
- View users' login history
- View a log of Identity Provider errors
- View users' training attendance

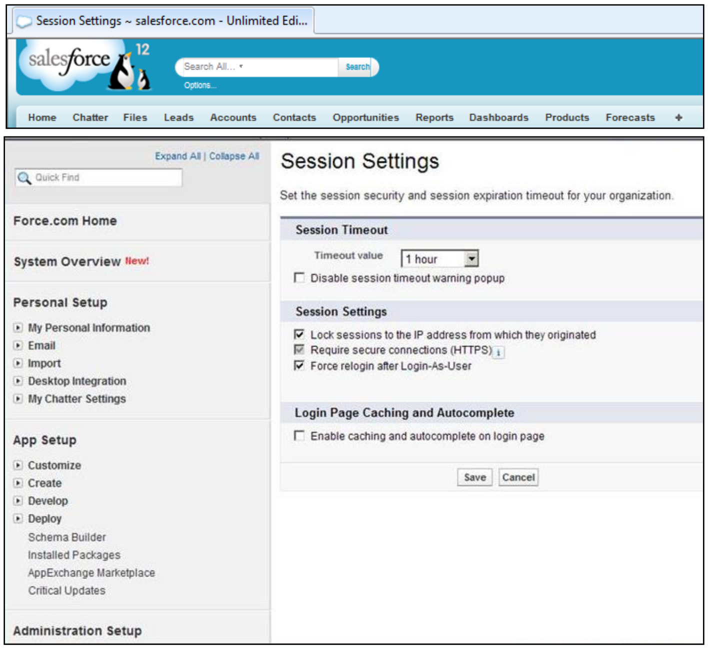
Figure 7-2 Administration Setup Configuration Family

The Administration Setup security configuration settings in the following table are named for the Individual Configuration area and the Sub-configuration area.

Configuration Family	Configuration Area	Sub-Group	Page Block
Administration Setup	Manage users	Roles	
		Profiles	
	Security Controls	Sharing Settings	
		Field Accessibility	
		Password Policies	
		Session Settings	
		Network Access	
		Package Support Access	
		Certificate and Key Management	
		Single Sign-On Settings	
		Identity Provider	
		View Setup Audit Trail	
		Expire All Passwords	
		Delegated Administration	
		Remote Site Settings	
		HTML Documents and Attachments Settings	
		Portal Health Check	
	Mobile Administration	Salesforce Mobile	Configurations
			Users and Devices
			Settings
		Chatter Mobile	Settings
			Users and Devices
		Mobile Dashboards	
	Desktop Configuration	Outlook Configuration Offline Briefcase Configurations Chatter Desktop Settings	
	Email Administration	Deliverability	
		Organization-Wide Addresses	
		Compliance BCC Email	
		Test Deliverability	
		Email to Salesforce	
		Delete Attachments Sent as Links	
		Email Footers	
	Google Apps	Settings	

Figure 7-3 Salesforce Security Relevant Sub-Groups

The actual settings are implemented by changing the field settings of the Subgroup page to the GSA required value (see the Salesforce Security Configuration Options file at the link below). Fields vary and can take the form of check boxes, radio buttons, pull-down menus or open text. The figure below shows the Sessions Settings sub-group page.



Session Settings

Set the session security and session expiration timeout for your organization.

Session Timeout

Timeout value: 1 hour

☐ Disable session timeout warning popup

Session Settings

☑ Lock sessions to the IP address from which they originated

☑ Require secure connections (HTTPS)

☑ Force relogin after Login-As-User

Login Page Caching and Autocomplete

☐ Enable caching and autocomplete on login page

Figure 7-4 Sub-group Page with Fields

The following settings provide a sample of the configuration options documented in the Salesforce Security Configuration Options Parameters at the link below.

SF Security Configuration Options

8 Salesforce User Permissions

An up to date listing of Salesforce out of the box Profiles can be found at Salesforce Standard Profiles. The standard profiles are not used by GSA teams.

9 External Customer Access

Government employees and contractors not credentialed within the GSA infrastructure, but still holding PIV compliant level of access within their own agency, will have a business need to have limited access to the GSA's Salesforce resources. There are several ways to accomplish this, depending on the level of risk to the information:

- Salesforce Communities and Portals: The Salesforce CRM customer community is true self-service software as a service (SaaS); designed so that external customers can help themselves to similar tools as internal users. Also, several levels of authentication are available via customer portals.

- Customer Chatter Groups: This method provides outside entities with access to Salesforce Chatter. This method is more targeted around a project or program, and not for general outreach. Customer Chatter Groups use 1Factor Authentication (1FA) for access. The group owner will be manager of the Chatter group and is responsible for implementing the policy that no documents will be posted in their respective group (policy enforcement outlined in SF guide) and must use SF access control. See section 10 for further detail.
- External Access Accounts: Are user accounts created on GSA's Active Directory "EXT" infrastructure which functions identically to GSA User Accounts and accesses Salesforce in the same way as an off-network GSA user would access it. Hence the account holder must comply with all HSPD-12 and GSA IT Security Policy. A proportional business case, appropriate adjudication and sufficient review time must be provided. Refer to Section 9.3, "External Access Accounts" for specifics.

9.1 Salesforce Customer Community Authentication

2Factor Authentication (2FA) Customer Community - Applications with external user access requirements of moderate data will be accessed via Salesforce Communities secured to 2FA using Login Flows or OMB MAX authentication. Organization owners are responsible for provisioning of the Communities and coordinating setup and support with the Salesforce COE (for two factor authentication).

1Factor Authentication (1FA) Customer Community – Applications with external user access requirements of low data will be accessed via 1FA Customer Communities. These Communities will use SF access control (all Authentication/Authorization/Accounting is handled by Salesforce). Low impact data verification is contained in the Application Review document, certified by the System ISSO and approved by the Application Owner, and ISSM. Password requirements for 1FA mandate at least 8 characters, including at least 1 number, 1 letter, and 1 special character.

9.2 Procedure to Acquire External Access Accounts

Anyone accessing GSA information systems that contain moderate impact data must be adjudicated fully under the HSPD-12 guidelines for that agency prior to being granted access to GSA systems. At a minimum this must be a NACI adjudication. If this requestor holds a National Security clearance or a Public Trust investigation higher than a NACI, the type and date of the adjudication must be indicated. This information is verified by the requesting Agency Security Officer and indicated by signatory authority from that Agency (which may be the assigned System ISSO, ISSM or HR personnel, according to that Agency's policy) on the "User Request Form Salesforce Template" attached to the request (see form template at the link below).

User Request Form Salesforce Template

9.3 Processing External Access Accounts

The Application Owner of the GSA Salesforce Application will submit via email a signed and completed “User Request Form Salesforce” to the applicable Regional ISSO (RISSO). RISSOs are identified at https://ea.gsa.gov/EAWEB/#!/RISSO_POC. Once the email is received, the RISSO will submit a Service Desk request for the account to be created. The ticket is then routed to the Directory Services Team who creates the account, and notes the “UserID” in the ticket and forwards that ticket to the “OCIO App Support” queue. The OCIO Application Support team then creates the user in Salesforce and sends an email to the external user, providing a carbon copy to the RISSO and the Application Owner. The “External Access to GSA Salesforce User Guide” at the link below must be attached to provide a bootstrap to the Salesforce application for the external user.

External Access to GSA SalesForce User

10 Scanning of the Salesforce Environments

The Force.com Security Source Code Scanner service (http://security.force.com/sourcescanner) provides custodians and developers of the Force.com platform information regarding the security of their code (specifically Apex and Visualforce) through next generation static analysis tools. The Salesforce code scanner service runs Checkmarx, a commercial scanning tool. GSA also hosts an internal Checkmarx tool for scanning Force.com. Due to reliability issues with the free Salesforce scanning service, all code scans of GSA Orgs are run using GSA’s internal tool. Scans are run using the “GSA_OCIO_SF_Preset” preset.

A code scan is performed only on the entire organization/sandbox, so that any error will be reflected upon any application within that organization/sandbox. The following process dictates the level of effort for the use of this vulnerability scanning service by organization:

- Development Sandboxes: when an app is first built, the developer does their code reviews by scanning it themselves.
- Quality Assurance (QA) Sandboxes: The QA team should do a scan of the app as part of their QA process to ensure it was coded properly before it gets pushed to UAT.
- User Acceptance Testing (UAT) Sandboxes: The System ISSO or System O&M runs the scan on behalf of the User Acceptance Testing process. That scan should be done once any expected changes have been completed. This development sandbox is also the PreProd/Staging/Integ sandbox.
- Production: All Salesforce System ISSOs shall provide a monthly scan report of their production Salesforce Environment Org to the OCISO via the email address saiso-salesforce-scan-reports@gsa.gov. Any Medium, High or Critical vulnerabilities shall be noted explicitly in the email, along with the business justification from the Application Review. Any High or Critical issues must be remediated within 30 days of discovery, and Medium issues within 60 days of discovery.

11 Customer Chatter Groups With External Access

Private Groups in Chatter allow users to segregate conversations, files and posts from the main GSA Chatter population. They allow teams, groups and partners to work together on projects and issues without worry that others might become privy to the information they share or post. Customer Chatter groups in GSA also allow for a feature not seen before in the Agency, that being, the ability of GSA users to collaborate in real time with Non-GSA employees. Examples of these people are other agency employees, vendors, customers and others GSA does business with on a daily basis. With Customer Chatter groups, a group owner can invite Non-GSA personnel to work as a collaborative team in private and have their work kept away from public Chatter feeds in Salesforce. Chatter group owners have the responsibility to ensure their group is maintained, monitored and the data shared among members is not sensitive or otherwise critical to GSA’s operations.

GSA users that wish to create a Customer Chatter Group that allows outside customer access must read and acknowledge the Rules of Behavior for GSA's Customer Chatter Groups with Outside Users. To complete and submit a Rules of Behavior (ROB) agreement, go to: https://sites.google.com/a/gsa.gov/private-chatter-groups/. Additionally, all members of a Customer Chatter Group must comply with GSA's IT Rules of Behavior for users (GSA Order CIO2104.1A). The GSA Order can be found at https://insite.gsa.gov/portal/content/533042. Private group owners are accountable for the actions of all group members and should ensure any member invited is made aware of the Customer Chatter Group Rules of Behavior as well as the GSA Order.

Private group owners are responsible for maintaining a list of all group members and their email addresses for audit purposes. As such, group, owners are responsible for daily auditing of the posts and files within their group, ensuring any unacceptable posts are immediately removed. An OCIO audit will be performed monthly by the System ISSO of randomly selected groups to capture a representative sample of the authorized groups. If any groups are found to be in non-compliance with the Rules of Behavior agreed to by group owners, the System ISSO will notify them to immediately remove that content and the System ISSO will follow up to ensure such content has been removed. Results of audit reviews and investigations will be coordinated within GSA’s incident response capability by creating an Initial and follow up report and submitting it to the OCISO. Any group found non-compliant with the above Rules of Behavior during periodic audits is subject to immediate deletion without prior notification.